

Q2
accessing the segment using the copy of the decryption key at the user location for the segment and a control process, the control process responsive to a user limitation to control distribution of the electronic information; [and]
destroying the copy of the decryption key at the user location [after] in response to said accessing [the segment];
displaying the decrypted segment in response to said accessing; and
destroying the decrypted segment in response to said displaying.

Q2
3. (Amended) A method of accessing first and second encrypted segments of an electronic document comprising [the steps of]:

retrieving, at the user location, a first encrypted segment of the electronic document;
receiving, from a key server, [(a)] a copy of a first decryption key for the first segment and [(b)] at least one user limitation assigned to the first segment and associated with the first decryption key;
accessing the first segment using the copy of the first decryption key for the first segment; and
at the user location, destroying the copy of the first decryption key for the first segment [as a precondition to];
receiving a decryption key for accessing a second segment of the electronic document after said destroying.

Please add the following claims for consideration by the Examiner:

Q3
--- 4. A method of viewing encrypted electronic information on a display, comprising:
retrieving, at a user location, a segment of encrypted electronic information;
receiving, from a remote server, a decryption key for the segment;
decrypting the segment using the decryption key;
destroying, at the user location, the decryption key in response to said decrypting;
displaying the segment as decrypted on the display; and
destroying, at the user location, the segment as decrypted in response to said displaying.

B2

⁴
4. The method of claim 4, further comprising providing an encrypted communication channel, wherein said receiving occurs over the encrypted communication channel.

⁵
5. The method of claim ³4, further comprising entering user identification information, said receiving being responsive to said user identification information representing at least one of an authorized user and authorized conditions.

⁶
6. The method of claim ³4, further comprising limiting access to the segment at the user location consistent with predetermined criteria associated with at least one of the segment and user identification information.

⁷
7. The method of claim ³4, further comprising changing the predetermined criteria associated with the segment and user identification information.

⁸
8. The method of claim ³4, further comprising destroying, at the remote server, the decryption key.

⁹
9. A method of encrypting information, comprising:
providing, at a user location, electronic information having at least one segment;
receiving, from a remote server, an encryption key for a segment of said at least one segment, the encryption key being associated with a decryption key;
associating at least one access precondition with the decryption key;
encrypting the segment with the encryption key;
destroying, at the user location, the encryption key and any unencrypted versions of said segment in response to said encrypting.

10.
11. The method of claim 10, further comprising performing said receiving, said associating, said encrypting, and said destroying for each of the at least one segment.

11.
12. The method of claim 10, further comprising communicating the at least one access precondition to the remote server.

12.
13. The method of claim 12, further comprising performing said receiving, said associating, said encrypting, said communicating, and said destroying for each of the at least one segment.

13.
14. The method of claim 10, said associating further comprising associating with the decryption key at least one of an authenticated user, a group name, time, date, day of week, and network address access precondition.

15. A method for limiting access to information, comprising:
generating, at a server, first and second encryption keys and associated first and second decryption keys, respectively;
first sending the first decryption key to a user location;
second sending the second decryption key to the user location after destruction, at the user location, of the first decryption key.

16. The method of claim 15, further comprising:
receiving user identification information;
each of said first and second sending being contingent upon said user identification information representing an authorized user under authorized conditions.

17. The method of claim 15, further comprising recording each instance of said first and second sending.